Prime Portraits

Zachary Abel
Department of Applied Mathematics, MIT
77 Massachusetts Avenue, Cambridge, MA 02138, USA

Abstract

We introduce a versatile method for finding prime numbers that display surprisingly intricate visual patterns—hypothetically, any desired pattern is possible, with only mild distortion. We use this method to locate several examples of large prime numbers that are, in and of themselves, self-referential works of art.

Prime Portrait Examples

The 16,129-digit number P_{mer} whose first few digits are shown in Figure 1 is a special prime number. It doesn't qualify as a Mersenne prime, since it definitely isn't one less than a power of two, but it *is* a "Mersenne" prime when looked at the right way. Indeed, looking is key! Imagine laying out its digits in a 127×127 grid in order[1] and coloring them by value as in Figure 2: all 9s are colored white, all 0s black, and so on. The result is shown in Figure 3—yes, this prime number shows the face of Marin Mersenne! No wonder the Great Internet Mersenne Prime Search didn't find it.

P_{mer} = 8887888787878787787787787777777777777767777777676766676666666666665656565556555555554545454544444
44444444444443444343434333433333387878787787877787777787777777777767676776766766666766666666665656565655
65555555555545554555454454544444443443443343433433433333333887888788787887878787877777777777777777777766766
76767666666666566656556565556555554555455445454444544444444444443443443334333343333888878878878778777877
77878777777767676767677767766666676766666666656566565555555555555545545445454444444444434434433434343433433
34333878787887887878778787877778777777777777766767677676666666666566565655656565655554554545454545444444
54444443443434343434343334333333387887878887878778787777877777777777767767776777676666666666666666665665565
55555555545545454545444544444444434443434343333343333433338888888787887887877787877878777777777767767676667
66766767666666665565656556556555555555455444544444444443443434343434343433433333333888788788787878787887787
777777877777777777777676776766666666666665666565555554544545454545455445444544454444444444344343 . . .

Figure 1: The first thousand digits of the 16,129-digit prime number P_{mer}.

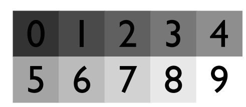

Figure 2: Digits are colored by value.

Let's look at a few more examples to begin to explore the range of possibilities for these *prime portraits*—and as an excuse for more (inexcusable) prime puns.

"Optimus" Prime. Figure 4 shows a 12,800-digit prime that transforms(!) into a recognizable figure when written in base 9, arranged in order in a 128×100 grid, and colored with the palette shown. (Why these colors? Why base 9? Simply because we can.)

Sophie Germain Prime. Mathematically, Sophie Germain primes (named after French mathematician Marie-Sophie Germain for her work relating to Fermat's Last Theorem) are those prime numbers p for which $2p + 1$ is also prime, such as 53 (because $2 \cdot 53 + 1 = 107$ is also prime). The 53×107-digit prime number P_{sg} in Figure 5 is not merely a punny "Sophie Germain" prime by virtue of depicting her; this number P_{sg} is actually a Sophie Germain prime! In other words, $2P_{\text{sg}} + 1$ is also prime!

Gaussian Prime. Gaussian integers are the complex numbers $a + bi$ where a and b are integers, and those that can't be factored (excluding ± 1 and $\pm i$ as factors) are called Gaussian primes. So 7 and $2 + 3i$ are Gaussian primes (try to factor them!), but $5 = (2 + i)(2 - i)$ and $5 + i = (1 + i)(3 - 2i)$ are not. If the left half of Figure 6 is read as a single 10,440-digit number A_{g}, and the right half likewise read as an integer B_{g}, then $A_{\text{g}} + iB_{\text{g}}$ is, visually and mathematically, a Gaussian prime.

[1] I.e., in standard English reading order: left-to-right, top-to-bottom. Nothing tricky here.

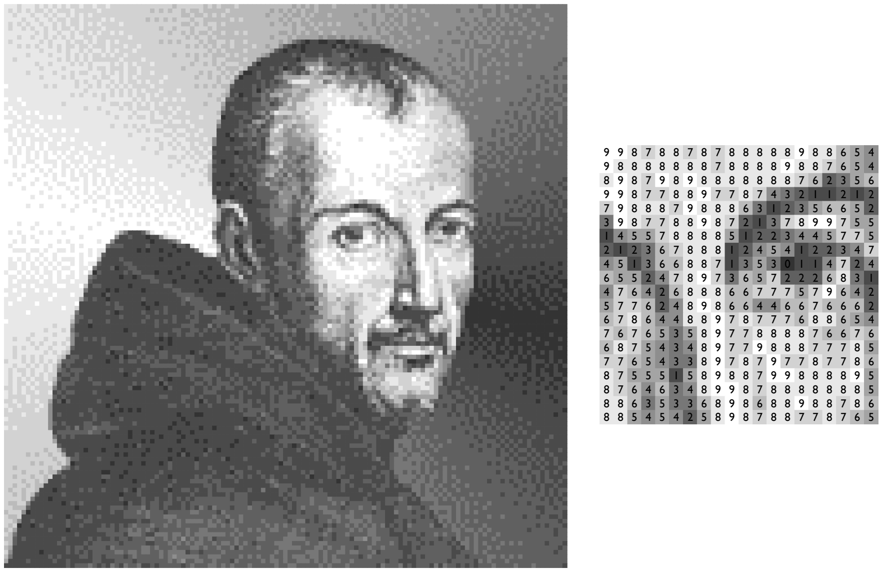

Figure 3: When gridded and shaded as in Figure 2, prime P_{mer} shows an image of Mersenne himself! Left: the full prime. Right: a closeup showing digits.

Twin Prime. A prime p is a twin prime if either $p+2$ or $p-2$ is also prime. The 1,271-digit primes P_{jack} and P_{finn} from Figure 7 are twin primes ($P_{\text{jack}}+2$ and $P_{\text{finn}}+2$ are both prime) showing images of Jack and Finn Harries of YouTube fame. In fact, more is true: primes that are 6 apart are called sexy primes (deriving from the Latin for 6), and since $P_{\text{jack}}+6$ and $P_{\text{finn}}+6$ are *also* prime, the numbers P_{jack} and P_{finn} are sexy[2] twin primes…

"Fermat" Prime. Our last example goes off-grid. The digits of the 5000-digit prime number P_{fer} have been positioned in order along the Fermat spiral (Figure 8), starting from the center and each rotated by an angle[3] of $\approx 137.508°$ from the previous to form an idealized phyllotaxis pattern. As Fibonacci numbers pervade this pattern, a portrait of Leonardo Bonacci (a.k.a., Fibonacci) would also have been appropriate.

How it Works

We still find the existence of these primes surprising—indeed, it's fun to consider that these primes existed long before their subjects were born! But mathematically, there are two simple principles driving all of the above examples: "Primes are everywhere," and "Primes are easy to spot (with a computer)."

Primes are Everywhere. A common strategy for locating large primes (e.g., for use in cryptographic schemes like RSA or Diffie Hellman) is to just choose randomly: to locate a prime with n digits, write down a random n-digit number, check if it's prime, and repeat until success. This strategy owes its effectiveness to the Prime Number Theorem, which ensures that each random sample has about a $1/(n \cdot \ln 10) \approx 1/(2.3n)$ chance of being prime, so we can expect to stumble into a prime after only about $2.3n$ trials. For a 16,129-digit prime like P_{mer}, only about 37,138 samples are required. (Note that this strategy relies on the *ubiquity* of primes, not just their *infinitude*—there are infinitely many powers of 2, for example, but they're far too spread out for a random search to reliably find them.)

We modified this strategy only slightly: instead of generating truly random numbers, we created candidate numbers that all resembled Mersenne. Specifically, we started with a proper image of Mersenne,

[2] Tatler magazine calls them "the hottest boys in the world" [2].

[3] This is the golden angle, the smaller of two circular arcs that divide the circle in the golden ratio $\phi = \frac{1}{2}(1+\sqrt{5})$.

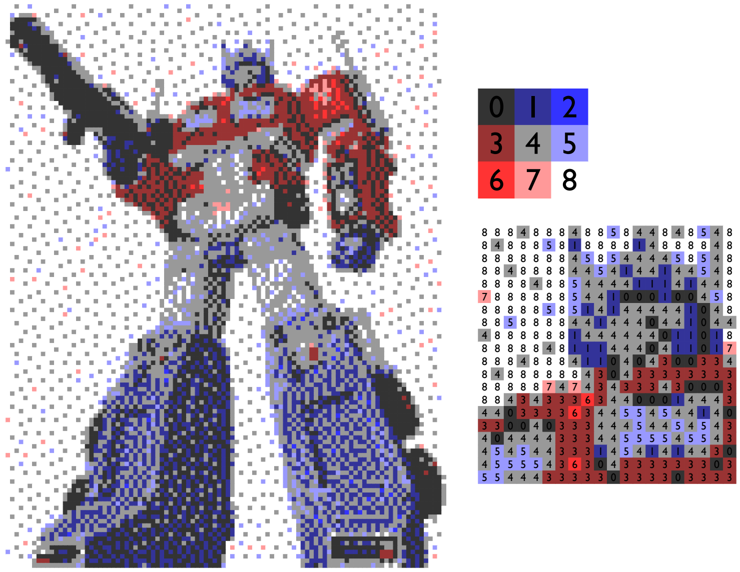

Figure 4: The 12,800-digit prime number P_{opt} has been written in base 9, arranged in a 128×100 grid, and colored with the palette shown in the top right.

Figure 5: The 5,671-digit prime P_{sg} has been drawn in a 107×53 grid. $2P_{\text{sg}} + 1$ is also prime.

used a dithering algorithm (Floyd-Steinberg dithering [1]) to approximate the image using only the allowed 10 shades of gray, and then checked the resulting number for primality. By adding subtle noise to the portrait (randomly changing each pixel value by an imperceptible $\pm 1\%$) before dithering, we generated many different pixellations of the same image—enough that one of them happened to be prime. Thankfully, it appears that the properties of "looking like Mersenne" and "being prime" are independent enough for the Prime Number Theorem's probabilities to still apply.[4] In principle, this same strategy can work for *any* target image.

Primes are Easy to Spot (with a Computer). In the procedure above, how do we *test* whether a given number is prime? Fast algorithms for primality testing do exist, but they require surprising subtlety. The widely used RSA cryptosystem relies on the infeasibility of factoring numbers with just a few hundred digits[5], even with today's best hardware and most advanced algorithms. In particular, the naïve method of trial division[6] is woefully outmatched by the 1,271 digits of P_{jack} or P_{finn}, to say nothing of the 16-thousand digits of P_{mer}. By contrast, software packages like the Gnu Multiple Precision Library (which we used) or Mathematica can test whether numbers of these sizes are prime in mere minutes, with clever techniques that test for primality without relying on factoring.

Furthermore, for numbers this large, the best general purpose algorithms are probabilistic, meaning they have a small (but tunable) chance of error. We ran 100 rounds of the Miller-Rabin test [3] on each of the above examples, making the chance of error less than 4^{-100} (smaller than the chance of winning the Powerball jackpot 7 times in a row!), discounting the possibility of hardware failure (which is more likely).

Acknowledgments

We are grateful to Jon Dobres, Scott Kominers, and Andrea Hawksley for helpful comments regarding this paper's presentation, and to Will Schwartz for suggesting many amusing prime puns, including the above

[4] Indeed, it would be stranger if they *were* somehow correlated!

[5] RSA public keys with 1024 or 2048 bits are common, corresponding to about 300 or 600 decimal digits.

[6] Trial division: "is it divisible by 2? by 3? by 5? ..."

twin primes example.

References

[1] Robert W. Floyd and Louis Steinberg. An adaptive algorithm for spatial grey scale. *Proceedings of the Society of Information Display*, 17:75–77, 1976.

[2] Sophia Money-Coutts. The ultimate twinset: Jack and Finn Harries! *Tatler*, 2013.

[3] Michael O. Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12:128–138, 1980.

Figure 6: The numbers A_{g} and B_{g}, forming a Gaussian prime $A_{\mathrm{g}} + i \cdot B_{\mathrm{g}}$, have each been drawn in 72×145 grids and tinted red and blue, respectively.

Figure 7: The 1,271-digit number P_{jack} (left), drawn here in a 41×31 grid, is such that P_{jack}, $P_{\mathrm{jack}}+2$, and $P_{\mathrm{jack}}+6$ are all prime, making P_{jack} a "sexy twin prime." The same is true for P_{finn} (right).

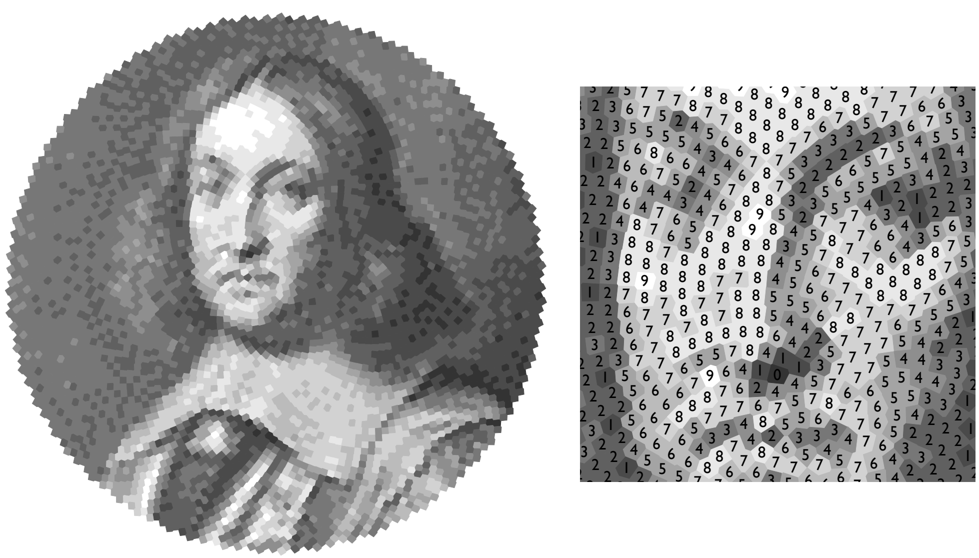

Figure 8: The $5{,}000$ digits of prime P_{fer} have been strung along the Fermat spiral.